Understanding & Avoiding Malware Script

PDF Terms of Use

This PDF version of this module is intended to be provided as an alternate format of transmission to licensed users of the KnowBe4 content only and may not be distributed beyond the licensed users, published anywhere that provides access beyond this group (including the Internet), or otherwise used outside of the terms of the subscription licensing agreement, including after the subscription ends. This PDF may also not be manipulated or modified. All images, text, and other assets are copyrighted by KnowBe4 and cannot be used in derivative works. Please refer to your master service agreement and/or subscription agreement for more information.

Section 1:
Slide 01 of 09: Introduction

Please note the menu at the bottom of the screen. This menu is available on each page to help you navigate this training.

You can navigate through this course by using a mouse or by using the tab and enter keys on your keyboard.

To proceed through this training, select the 'previous slide button' or the 'next slide button'.

If you need help at any time with the way this course functions, select the help button.

We have provided a PDF glossary that can be opened in a new tab at any time by selecting the glossary button.

“The Many Faces of Malware” button opens a further learning section of the training and can be accessed at anytime.

This slide and the opening slide contain a link to a PDF version of the entire course script that can be opened in a new tab by selecting the full script button. On all other slides, the slide script can be accessed within the slide only, and can be opened by selecting the slide script button. The script scroll bar can be navigated using a mouse or by using the tab and up/down arrows on your keyboard.

A quiz follows this training. After choosing your answer(s), submit your response(s) by selecting the submit button.

Slide 02 of 09: Help

You can navigate through this training by using a mouse or by using the tab and enter keys on your keyboard. To proceed through this training, select the previous slide button (‹) or the next slide button (›). If you need help at any time with the way this training functions, select the help button. We have provided a PDF glossary that can be opened in a new tab at any time by selecting the glossary button. This slide, and the introduction slide contain a link to a pdf version of the of the entire course script that can be opened in a new tab by selecting the full script button. On all other slides, the script can be accessed within the slide only, and can be opened by selecting the slide script button. The script scroll bar can be navigated using a mouse or by using the tab and up/down arrows on your keyboard. A quiz follows this training. After choosing your answer(s), submit your response(s) by selecting the submit button.

Slide 03 of 09: Gatekeepers: Protecting Private Information and Access

Welcome

Slide 04 of 09: Malware in the Wild

Imagine you work at a hospital and suddenly every computer you use for vital services locks up. You no longer have access to patient medical records, CT scans, lab work, etc. All medical data normally collected by the hospital's systems must now be handwritten, and all pharmaceutical requests must be faxed. After several days of this, the hospital has no choice but to transfer the majority of their patients to other hospitals and turn away all new patients. The situation causes extreme stress for doctors, nurses, receptionists, and, of course, patients who could be facing life-threatening circumstances.

Sounds like a nightmare, right? Unfortunately, it's a real story that has been played out over and over again, at several hospitals around the world, as a result of ransomware—a cyber-attack that encrypts systems and files until a specific ransom is paid. Ransomware is just one example of how malicious software presents an ongoing threat that every organization in every industry must defend against.

Slide 05 of 09: What Can Malware Do?

When cities, hospitals, and other entities don't have access to their systems—which is the case when falling victim to a ransomware attack—the impacts can be felt by millions of people. The city of Atlanta, Georgia offers a prime example of this. For several days their computers were locked up by cybercriminals, which crippled basic municipal services. When this happens to hospitals—an all too common occurrence—the results can be life threatening.

The same is true for industrial plants. If malware were to successfully infect computers that control equipment safeguards, there's a good chance the machines would be over-worked and damaged—the plant could even explode. This exact thing happened at a steel mill in Germany when a blast furnace couldn't be shut down. Imagine that same scenario playing out over our critical infrastructure such as dams, traffic control, water distribution, power stations, and other systems that millions of people rely on every day.

Some malware is designed to infiltrate a network and open backdoors to steal data without detection. Other types hit consumers, such as an incident in India where several ATMs were infected with malware that stole cardholder data—including PINs and account numbers.

In short, the damage malware can inflict is seemingly limitless.

Slide 06 of 09: Catching Malware

How does malware end up on computers and networks across the globe? Most often it's because of human error. Someone clicks on a malicious link, downloads a malicious attachment, plugs a random USB device or flash drive into their computer, fails to update systems with critical security patches, misconfigures a network setting (inadvertently leaving a backdoor open), or falls for a social engineering scam and divulges confidential data, leading to more attacks.

Of course, it's not always human error. In a few cases, well-funded, highly sophisticated groups of cybercriminals leverage their resources to break into networks without much human interaction. But most of the time, malware infections result from mistakes, not machines.

Slide 07 of 09: Symptoms of an Infection

Because malware comes in many forms, symptoms will vary. Common signs include: a sluggish computer, lack of storage space, frequent crashes or freezes, sudden pop-ups and annoying unwanted programs, or even an increase in spam. The most dangerous forms of malware, however, normally go undetected for a long period of time.

Slide 08 of 09: Preventing Malware

Before going into malware prevention techniques, let's focus on one of the most important security awareness action items—following policy. Following our organization's policy means committing to the security of our employees, customers, clients, and business associates. Circumventing policy for any reason undermines our efforts to prevent cybercrime and could lead to security breaches. If you ever have any questions or need more information about our policies, please ask!

With that in mind, here are a few best practices to help prevent malware infections. Some of these will only apply to your personal life, but don't forget that cybercriminals target individuals as much as organizations.

Think before you click. Most malware infections are made possible by malicious links and attachments sent via email. Hover over the links to display the full URL, and avoid downloading random attachments. Stay alert for common phishing indicators such as poor grammar, threatening language, and urgent calls to action.

Never plug in random USB devices or flash drives. Social engineers can infect those devices with malware and leave them in public areas hoping to take advantage of someone's curiosity.

Keep systems and devices up to date. Consider enabling automatic updates whenever possible so you never miss an important security patch.

Keep your antivirus and anti-malware software up to date on all of your devices. Even the free options help prevent potential infections.

Back it up. Maintaining up-to-date backups of your data won't prevent malware, but if a device or computer becomes infected, you will at least have an easier path to recovery. Backups are especially important when encountering ransomware attacks.

Surf with caution. Unfortunately, cybercriminals often compromise legitimate websites. If you receive a sudden popup that claims your computer has been infected or asks you to update your browser—don't click on it! Also keep an eye out for malvertising—malicious ads that are injected into legitimate websites.

Routinely audit software and apps. Over time, we install programs and then forget about them—especially with smartphones. Make a habit of auditing your apps and removing any that you don't use regularly. While you're at it, double-check the security settings and permissions of apps to ensure they have the minimum amount of access necessary to function.

Do your research before installing anything. App stores are littered with malicious or imposter applications that infect devices with malware. Always research developers before downloading apps or programs, and only download them from legitimate sources.

Stay away from illegal file-sharing or streaming services. These services are breeding grounds for malware. If you can't prove the developer is legitimate, find a different source.

Report anything unusual. An unknown person hanging around, a random USB device in the parking lot, a phishing email, a scammy phone call, a computer acting strangely—anything that raises your suspicions should be reported immediately!

Slide 09 of 09: Wrap Up

All it takes for malware to compromise our organization is a hasty click or momentary lapse in awareness. That's why it's important for every member of our organization to stay alert at all times, and take extra precautions to ensure the confidentiality, integrity, and availability of our systems and networks.

We thank you for taking this awareness course. Your commitment to security is an invaluable resource in our battle against cybercrime. Now let's see what you've learned about malware with a short quiz.

Section 2:

Slide 01 of 01: The Many Faces of Malware

Some variants of malware steal confidential data or spy on individuals by secretly accessing cameras and microphones. Others lock up systems and encrypt files. Some strains physically damage equipment and facilities. And while the consequences of an infection may vary in severity, it's imperative that our organization circumvents any and all cyber-attacks and the malicious software they hope to distribute. To learn more about the various types of malware, click on each icon.

Adware: Adware is typically the least dangerous form of malware—it merely displays ads on your screen.

Spyware: Spyware tracks your internet activities and sends Adware back to your system. It can also turn on your camera and microphone without your knowledge.

Viruses: Viruses self-replicate by injecting malicious code into other programs and apps installed on your computer or device.

Worms: A worm is a program that replicates itself—some destroy data and files, others just clog computer resources.

Trojans: A Trojan horse can be used for a variety of malicious purposes. Modern versions are used to open digital "backdoors", providing unauthorized access to a network.

Keyloggers: Keylogger software can record and transmit everything typed on a computer, allowing the attacker to steal login credentials and other sensitive information.

Scareware: Scareware uses fear tactics with sudden pop ups that claim the user's computer has been infected, then prompts them to install (malicious) software to remove the infection.

Ransomware: Ransomware encrypts your computer or files until a ransom is paid. If you don't pay the ransom by a certain date, the files will be destroyed.